UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/522,067	10/04/2005	Christopher Ian Blake	BLAKE	7581

23643 7590 02/08/2008
BARNES & THORNBURG LLP
11 SOUTH MERIDIAN
INDIANAPOLIS, IN 46204

EXAMINER	
CHAI, LONGBIT	
ART UNIT	PAPER NUMBER
2131	
MAIL DATE	DELIVERY MODE
02/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/522,067	**Applicant(s)** BLAKE, CHRISTOPHER IAN	
	Examiner Longbit Chai	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 January 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-9,11-16,18-28,32 and 33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-9,11-16,18-28,32 and 33* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 January 2005* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *1/3/2008*.
4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

1. At present, the pending claims are 1 – 3 – 9, 11 – 16, 18 – 28, 32 and 33.

Response to Arguments

2. Applicant's arguments with respect to the instant claims have been fully considered but are moot in view of the new ground(s) of rejection as the primary reference (WO 99/56429).

3. As per claim 1 (for the portion of the original prior-art U.S. Patent 5,991,410 used as the 2nd reference), Applicant asserts Albert does not teach "a high security module located remotely from the smartcard reader (*see response below*) and at an inaccessible location relative to the smartcard reader" (Remarks: Page 6, 2nd Para). Examiner notes Applicant's argument has no merit since the alleged limitation "and at an inaccessible location" has not been recited into the claim. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

4. Furthermore, as per claim 1 (for the portion of the original prior-art U.S. Patent 5,991,410 used as the 2nd reference), Applicant further asserts Albert does not teach "a high security module at a remote location translating an encrypted signal to another format useable by the access controller" (Remarks: Page 6, 3rd Para). Examiner respectfully disagrees because Albert teaches (a) the authorization processor 600 then performs database activities and/or contacts a computer of the issuer of the credit card to obtain either an authorization or denial of the transaction (Albert: Figure 2 and Column 7 Line 18 – 21: the authorization processor 600 is qualified as a remote high security module) and the settlement / authorization processor 600 then presents to the credit card issuers, in a format acceptable to each credit card issuer, data

records indicative of the data frames received from the terminal. The credit card transactions are thereby posted to the accounts of the credit card cardholders, to reflect the charges posted onto these accounts (Albert: Figure 2 and Column 8 Line 63 – 65: translated into another signal format acceptable by the card issuer) – Examiner notes this is also consistent with the disclosure of the instant specification "The HSM 904 translates the encrypted signal to another format for a controller and communicates the translated signal to the access controller 906. The translation preferably involves **decrypting** the message to obtain the security or access information from the smartcard, e.g. "Facility Code" and the "Access number" and communicating the values to the access controller" (SPEC: Page 19 / Line 1 – 6).

Claim Objection

5. Claims 1 and 16 are objected to because of the following informalities: "said transmitting signal" should be replaced with "said transmitting said encrypted signal". Appropriate corrections are required. Any other claims not addressed are objected by virtue of their dependency should also be corrected.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 3 – 8, 16, 18 – 23, 27, 32 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scott et al. (WO 99/56429), in view of Albert et al. (U.S. Patent 5,991,410).

As per claim 1 and 16, Scott teaches a method of providing secure transmissions from a biometric smartcard reader (Scott: Page 4 / Line 29 – 32 and Figure 4A – 4D & Figure 1), said method comprising the steps of:

encrypting a signal created by said biometric smartcard reader dependent on a smartcard containing biometric data, said smartcard reader able to obtain biometric data directly, said signal comprising access information dependent upon biometric data obtained directly by said biometric smartcard reader from a user and said biometric data contained in said smartcard (Scott: Page 4 / Line 29 – 32, Page 13 / Line 27 – 32, Page 4 / Line 1 – 3 and Figure 1 & Figure 4A – 4D: (a) a biometric smartcard reader is included as part of the portable personal identification device and (b) the processing unit 16 including a processor circuit, a memory and an encoder (encryption unit) also provides the function of a smart card reader (Scott: Page 4 Line 1 – 3: i.e. in the middle section of PID device (Figure 1 / Element 2) and the encoder provides the encrypting function);

transmitting said encrypted signal to a high security module at a remote location relative to said smartcard reader (Scott: Page 4 Line 3 / Line 22 – 28 and page 4 Line 14 – 18: the processing unit of the card reader encrypts the verification signal and transmit to the remote host system – the decrypting unit of the remote system is qualified as a high security module at a remote location);

However, Scott does not teach translating by said high security module at said remote location said transmitted signal to another format useable by an access controller; and controlling an access mechanism using said access controller dependent upon said translated signal.

Albert teaches translating by said high security module at said remote location said transmitted signal to another format useable by an access controller (Albert: Figure 2, Column 7 Line 18 – 21 and Column 8 Line 63 – 65: the authorization processor 600 then performs database activities and/or contacts a computer of the issuer of the credit card to obtain either an authorization or denial of the transaction (Albert: Figure 2 and Column 7 Line 18 – 21: the authorization processor 600 is qualified as a high security module) and the settlement / authorization processor 600 then presents to the credit card issuers, in a format acceptable to each credit card issuer, data records indicative of the data frames received from the terminal. The credit card transactions are thereby posted to the accounts of the credit card cardholders, to reflect the charges posted onto these accounts (Albert: Figure 2 and Column 8 Line 63 – 65: translated into another signal format acceptable by the card issuer) – Examiner notes this is also consistent with the disclosure of the instant specification "The HSM 904 translates the encrypted signal to another format for a controller and communicates the translated signal to the access controller 906. The translation preferably involves decrypting the message to obtain the security or access information from the smartcard, e.g. "Facility Code" and the "Access number" and communicating the values to the access controller" (SPEC: Page 19 / Line 1 – 6); and

controlling an access mechanism using said access controller dependent upon said translated signal (Albert: Column 7 Line 18 – 21: based on the translated signal received from said authorization processor at said host computer signals to determine the authorization or denial of a transaction – i.e. access control mechanism).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Albert within the system of Scott because (a) Scott teaches a portable personal identification device including a biometric smartcard reader for providing secure access to a remote host facility (Scott: Abstract) (b) Albert teaches an effective and convenient mechanism associated with a financial transaction device that reads the identifying data from a biometric smart card and translating the signal into a acceptable format to a 3rd-party authority as for authentication purpose (Albert : Figure 2, Column 7 Line 18 – 21 and Column 8 Line 63 – 65).

As per claim 3 and 18, Scott as modified teaches said biometric data comprises fingerprint data (Scott: Page 4 / Line 29 – 32, Page 13 / Line 27 – 32, Page 4 / Line 1 – 3).

As per claim 4 and 19, Scott as modified teaches said biometric data is not transmitted to said high security module at said remote location from said smartcard reader (Scott: Page 2 Line 11 – 12, Page 4 Line 3 / Line 22 – 28 and page 4 Line 14 – 18: only if the verification is successful).

As per claim 5 and 20, Scott as modified teaches providing access using said access mechanism if said translated signal is determined by said access controller to authorize access (Albert: Column 18 Line 62 – 67: the recovered digital data signal format is communicated with authorization processor to authorize access).

As per claim 6 and 21, Scott as modified teaches said access mechanism is able to provide access to at least one of a door, portal, computer, network, secure equipment and secure installation (Albert: Column 18 Line 62 – 67).

As per claim 7 and 22, Scott as modified teaches said access information comprises at least one of a person's name, a facility code, a company code, an access code, and an issue code (Albert: Column 5 Line 24 – 29).

As per claim 8 and 23, Scott as modified teaches said signal is encrypted using triple DES, Skipjack, or AES Rijndael encryption (Albert: Column 12 Line 40).

As per claim 14 and 27, Albert teaches said translated signal is in a controller-specified format (Albert: Column 8 Line 62 – 65).

As per claim 32, Scott as modified teaches said encrypted signal is transmitted using a communications protocol and said high security module decrypts said transmitted signal, said communications protocol being different from said format useable by said access controller (Albert: Column 18 Line 49 – 61 and Column 8 Line 62 – 67).

As per claim 33, Scott as modified teaches said transmitted signal is transmitted using one of RS-232 and RS-485 communications protocol (Examiner notes Official Notice is taken that the use of either RS-232 or RS-485 communications protocol is a well-known typical communication protocols).

7. Claims 9, 11 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scott et al. (WO 99/56429), in view of Albert et al. (U.S. Patent 5,991,410), and in view of Baratelli (U.S. Patent 6,325,285).

As per claim 9 and 24, Scott as modified does not disclose expressly encrypting communications between said biometric smartcard and said biometric smartcard reader.

Baratelli teaches encrypting communications between said biometric smartcard and said biometric smartcard reader (Baratelli: Column 6 Line 46 – 55 and Column 7 Line 35 – 44: the information between the smart card and WRU (Write / Read Unit) of a smart card is encrypted using private / public key mechanisms).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Baratelli within the system of Scott as modified because (a) Scott teaches a portable personal identification system including a biometric smartcard reader for providing secure access to a remote host facility (Scott: Abstract), and (b) Baratelli teaches an enhanced security mechanism of smart card system by first validating a biometric identity of an individual and subsequently encrypting the secure data with security keys for authentications (Baratelli : Column 1 Line 40 – 46 and Column 6 Line 46 – 55).

As per claim 11, Scott as modified teaches said high security module translates said encrypted signal to said other format (Albert: Figure 2, Column 7 Line 18 – 21 and Column 8 Line 63 – 65: the settlement / authorization processor 600 then presents to the credit card issuers, in a format acceptable to each credit card issuer, data records indicative of the data frames received from the terminal. The credit card transactions are thereby posted to the accounts of the credit card cardholders, to reflect the charges posted onto these accounts (Albert: Figure 2 and Column 8 Line 63 – 65: translated into another signal format acceptable by the card issuer) – Examiner notes this is also consistent with the disclosure of the instant specification "The HSM 904 translates the encrypted signal to another format for a controller and communicates the translated signal to the access controller 906. The translation preferably involves decrypting the message to obtain the security or access information from the smartcard, e.g. "Facility Code" and the "Access number" and communicating the values to the access controller" (SPEC: Page 19 / Line 1 – 6).

8. Claims 12 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scott et al. (WO 99/56429), in view of Albert et al. (U.S. Patent 5,991,410), in view of Baratelli (U.S. Patent 6,325,285), and in view of Delp et al. (U.S. Patent 6,922,558).

As per claim 12 and 25, Scott as modified does not disclose expressly said smartcard reader and said high security module are separated by a distance of up to 1.2 kilometers.

Delp teaches said smartcard reader and said high security module are separated by a distance of up to 1.2 kilometers (Delp: Column 18 Line 57 – 59: the maximum distance for 4000 feet = (0.3 m / ft.) x 4000 ft. = 1.2 km).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Delp within the system of Scott as modified because (a) Scott teaches a portable personal identification system including a biometric smartcard reader for providing secure access to a remote host facility (Scott: Abstract), and (b) Delp teaches providing various network infrastructures for a vender tracking at remote host system that can increase the total number of modules supported by the system and thus increase the coverage area including remote locations with cost reductions for installation and maintenance (Delp: Column 17 Line 21 – 25, Column 18 Line 62 – 67 and Abstract / Line 18 – 22).

9. Claims 13 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scott et al. (WO 99/56429), in view of Albert et al. (U.S. Patent 5,991,410), and in view of Baratelli (U.S. Patent 6,325,285), and in view of Bartholomew et al. (U.S. Patent 5,724,417).

As per claim 13 and 26, Scott as modified does not disclose expressly said smartcard reader and said high security module are separated by a distance of up to 15 meters.

Bartholomew teaches said smartcard reader and said high security module are separated by a distance of up to 15 meters (Bartholomew : Column 4 Line 37 – 38 / Line 47 – 50: signal coverage over distances on the order of tens or hundreds of feet and thus includes 50 feet = (0.3 m / ft.) x 50 ft. = 15 meters).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bartholomew within the system of Scott as modified because (a) Scott teaches a portable personal identification system including a biometric smartcard reader for providing secure access to a remote host facility (Scott: Abstract), and (b) Bartholomew teaches providing a smart card wireless data communication capabilities with a remote host system providing spanning moderate coverage distances (Bartholomew : Column 4 Line 37 – 50).

10. Claims 15 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scott et al. (WO 99/56429), in view of Albert et al. (U.S. Patent 5,991,410), and in view of Renner et al. (U.S. Patent 6,223,984).

As per claim 15 and 28, Scott as modified does not teach said controller-specified format is Wiegand format, or clock and data.

Renner teaches said controller-specified format is Wiegand format, or clock and data (Renner: Column 4 Line 9 – 11 and Column 6 Line 11 – 15: Wiegand format)

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Renner within the system of Scott as modified because (a) Scott teaches a portable personal identification system including a biometric smartcard reader for providing secure access to a remote host facility (Scott: Abstract), and (b) Renner teaches an effective mechanism to resolve the format compatibility issues across different remote authorization centers that may be implemented with various verification signal formats (Renner : Column 2 Line 23 – 32 and Column 3 Line 49 – 53).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Longbit Chai Ph.D.
Patent Examiner
Art Unit 2131
01/30/2008